Amendment to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (previously presented): A computer network comprising:

a first edge device coupled to a first physical private network, the first edge device configured to create a first table with information of a group of one or more virtual private networks reachable through the first edge device, the first table being stored in a first database;

a second edge device coupled to a second physical private network, the second edge device configured to create a second table with information of the group of one or more virtual private networks reachable through the second edge device, the second table being stored in a second database;

wherein, the first and second edge devices enable secure communication between the first and second physical private networks, and the first edge device shares the information of the group of one or more virtual private networks of the first table with the second edge device and the second edge device shares the information of the group of one or more virtual private networks of the second table with the first edge device.

Claim 2 (previously presented): The computer network of claim 1, wherein the first edge device includes logic for:

receiving a new route information;

storing the new route information in the first database; and

transmitting a portion of the new route information to the second edge device.

Claim 3 (previously presented): The computer network of claim 2, wherein the portion of the new route information is a route name.

Claim 4 (previously presented): The computer network of claim 2, wherein the second edge device includes logic for:

receiving the portion of the new route information;

accessing the first database based on the portion of the new route information;

retrieving the new route information from the first database; and

storing the retrieved route information in the second database.

Claim 5 (previously presented): The computer network of claim 1, wherein communication between the first and second physical private networks is managed according to a security policy associated with the networks.

Claim 6 (previously presented): The computer network of claim 5, wherein the security policy is defined for a security policy group providing a hierarchical organization of the security policy group, the security policy group including virtual private networks, users allowed to access the virtual private networks, and a rule controlling access to the virtual private networks.

Claim 7 (previously presented): The computer network of claim 6, wherein each of the one or more virtual private networks has full connectivity with all other virtual private networks and the security policy defined for the security policy group is automatically configured for each connection.

Claim 8 (previously presented): The computer network of claim 6, wherein the security policy provides encryption of traffic among the one or more virtual private networks and the rule is a firewall rule providing access control of the encrypted traffic among the one or more virtual private networks.

Claim 9 (previously presented): In a computer network including a first edge device coupled to a first physical private network and a second edge device coupled to a second physical private network, the first and second edge devices enabling secure

communication between the first and second physical private networks, a method for gathering virtual private network membership information comprising:

creating a first table with information of a group of one or more virtual private networks reachable through the first edge device,

storing the first table in a first database;

creating a second table with information of the group of one or more virtual private networks reachable through the second edge device;

storing the second table in a second database;

sharing the information of the group of one or more virtual private networks of the first table with the second edge device; and

sharing the information of the group of one or more virtual private networks of the second table with the first edge device.

Claim 10 (previously presented): The method of claim 9 further comprising:

receiving a new route information;

storing the new route information in the first database; and

transmitting a portion of the new route information to the second edge device.

Claim 11 (previously presented): The method of claim 10, wherein the portion of the new route information is a route name.

Claim 12 (previously presented): The method of claim 10 further comprising:

receiving the portion of the new route information;

accessing the first database based on the portion of the new route information;

retrieving the new route information from the first database; and

storing the retrieved route information in the second database.

Claim 13 (previously presented): The method of claim 9, wherein communication between the first and second physical private networks is managed according to a security policy associated with the networks.

Claim 14 (previously presented): The method of claim 13 further comprising defining the security policy for a security policy group, the security policy group providing a hierarchical organization of the security policy group including one or more virtual private networks, users allowed to access the one or more virtual private networks, and a rule controlling access to the one or more virtual private networks.

Claim 15 (previously presented): The method of claim 14, wherein each of the one or more virtual private networks has full connectivity with all other virtual private networks and the security policy defined for the security policy group is automatically configured for each connection.

Claim 16 (previously presented): The method of claim 14, wherein the security policy provides encryption of traffic among the virtual private networks and the rule is a firewall rule providing access control of the encrypted traffic among the virtual private networks.